



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/583,452	05/30/2000	Daniel R. Zaharris	M-8376-US	1693

7590 05/27/2004

Theodore P. Lopez  
MACPHERSON KWOK CHEN & HEID LLP  
2001 Gateway Place  
Suite 195E  
San Jose, CA 95110

EXAMINER
----------

NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/27/2004

18

Please find below and/or attached an Office communication concerning this application or proceeding.

1724

# Office Action Summary

Application No.

09/583,452

Applicant(s)

ZAHARRIS ET AL.

Examiner

Abdulhakim Nobahar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 24 May 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-3 and 6-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3 and 6-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

***Response to Arguments***

1. This communication is in response to applicant's amendment received on March 24, 2004.
2. The amendments to the specification are acknowledged.
3. The amendments to claims 1, 2, 7-11, 13 and 14 are acknowledged and that these amendments do not introduce any new matter to the claimed invention.
4. The cancellation of claims 4 and 5 and withdrawal of claims 22-25 are acknowledged.
5. Applicant's arguments have been fully considered but they are not persuasive.
6. Applicant on page 10, lines 11-13, argues "a DVD drive that merely transferred the data key and the medium key without encryption would leave the content vulnerable to hacking."

On the contrary, Angelo teaches that the DVD drive after querying the data key and the medium key from the disk, encrypts them and then transfers them to the system memory (see Fig. 3, blocks 54, 60 and 64).

7. Applicant on page 10, second paragraph, argues "this combination key is NEVER stored on the storage medium as disclosed in Angelo. ... As such, the method recited in claim 1 is superior to that disclosed in Angelo. ..."

Angelo discloses the generation of a DVD drive key (corresponding to the recited an internal key) (col. 4, lines 5-10). Angelo further discloses that the DVD drive combines the disk key and the media key to generate an encrypting disk/media key (corresponding to the recited generating a combination key) (col. 4, lines 42-46) and then this combination key is used to decrypt the information on the medium (col. 4, lines 65-67). Thus, in a broad interpretation Angelo discloses the same features and limitations of claim 1 of the invention.

8. Applicant on page 10, lines 10-14, with respect to claim 14 argues "For example, those reference make no teaching or suggestion for the provision of a plurality of combination keys from the plurality of medium keys and the plurality of internal keys...."

Angelo discloses that when a plurality of program information is recoded on a medium, each of the program information has its own associated disk key and media key (col. 4, lines 42-56). Thus, according to the discussion stated above for claim 1 a plurality of combination keys would be generated to decrypt the plurality of program information on the medium.

9. In light of the above submission the previous rejection of claims 1-3, and 6-21 is maintained as follows.

***Previous rejection:***

***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

1. Claims 1-3, 8, 9, 14, 16, 17, 19 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Angelo et al. (5,932,754) (Angelo).

2. Referring to claim 1, Angelo discloses a method for decrypting protecting data recorded on a medium such as a DVD disk (col. 1, lines 57-67). Angelo also discloses the generation of a key every time a DVD system is powered on (col. 4, lines 7-8), a media key stored on the DVD disk is retrieved by the DVD drive and a combination key

Art Unit: 2132

is generated (col. 4, lines 42-47). Angelo further discloses that the combination key is used to decrypt the data on the disk (col. 4, lines 65-67).

3. Referring to claim 2, Angelo discloses that the DVD controller of the DVD system decrypts the encrypted key,  $d_k$ , that corresponds to the recited master media key (col. 3, lines 13-22 and col. 4, lines 59-61). Angelo also discloses that a unique drive key corresponding to the medium key is calculated from the disk key corresponding to the recited master media key stored on the disk (col. 4, lines 5-7).

4. Referring to claim 3, Angelo discloses that the DVD system keys (internal key) are generated randomly (col. 2, lines 1-14 and col. 3, lines 1-12).

5. Referring to claims 8 and 9, Angelo discloses that a DVD disk may contain a variety of encrypted sections of information (i.e., different area with different data) each with its own particular key (col. 4, lines 50-56). In such a case a plurality of disk keys (additional keys) would be generated as stated in the case of claim 1 above.

6. Referring to claims 14 and 20, Angelo discloses:

Generating a plurality of internal keys using a pseudo-random number generator (data storage engine). See col. 4, lines 7-8, col. 2, lines 1-14 and col. 3, lines 1-12.

Decrypting a master media key and a file system structure corresponding to a first portion of the data using at least one internal key. See col. 3, lines 13-22 and col. 4, lines 50-61.

Generating a plurality of medium keys from the master media key. See col. 4, lines 5-7.

Art Unit: 2132

Generating a plurality of combination keys from the plurality of medium keys and the plurality of internal keys. See col. 4, lines 42-56.

Decrypting a first portion of the data using a first combination key. See col. 4, lines 65-67.

Encrypting a portion of data using said first combination key and storing the portion on the storage medium. See col. 60-67, col. 2, lines 40-45 and col. 3, lines 48-63.

7. Referring to claims 16, 17 and 19, Angelo discloses that DVD disk may contain different encrypted data recorded in different area of the disk each section with its own associated key that is used for the encryption of data and the combination key for decryption (col. 2, lines 41-50 and col. 4, lines 50-56).

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 6, 7, 10-13, 15, 18 and 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (5,932,754) (Angelo) in view of Silverbrook et al. (6,334,190 B1) (Silverbrook).

3. Referring to claim 6, Angelo does not disclose the use of exclusive OR function to generate the combination key. Silverbrook teaches the use of exclusive OR function in the encryption process to provide a greater security (col. 4, lines 15-40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the two encryption keys by using exclusive OR function as taught in Silverbrook in the method of Angelo, because it would provide a much higher level of protection and security for the secure data (col. 1, lines 25-31).

4. Referring to claims 7, 18 and 21, Angelo discloses that different data may be recorded on different area of a DVD disk and each portion of data encrypted and decrypted with particular keys using any type of cryptography technology (col. 4, lines 50-56). But Angelo does not expressly disclose the use of DES and triple DES for decryption and encryption. Silverbrook discloses the use of DES standard for encryption and decryption (col. 3, lines 64-67) and specifically the use of triple DES for more security (col. 4, lines 7-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to utilize triple DES for encryption and decryption instead of single DES as taught in Silverbrook in the system of Angelo, because it would provide a much higher level of protection and security for the secure data (col. 1, lines 25-31).

5. Referring to claims 10, 11 and 13, these claims are rejected as applied to the like elements of claims 1, 4, 6 and 9 as stated above.



6. Referring to claim 12, Angelo discloses any number of different encrypted data can be recorded on the DVD disk (col. 4, lines 50-560) and any cryptosystem type and encryption key can be applied to the recorded information (col. 3, lines 1-22).

7. Referring to claim 15, Angelo does not expressly disclose the use of a pseudo-random number generator comprising a logical feedback shift register (LFSR) and a seed for the LFSR. Silverbrook teaches the use of a pseudo-random number generator having LSFR (col. 11, line 60col. 12, line 15) to generate encryption keys. Silverbrook further teaches the use of a specific seed by the pseudo-random number generator (col. 4, line 7-col. 8, line 10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to utilize a LFSR pseudo-random number generator that uses a seed value as taught in Silverbrook in the system of Angelo, because it would provide a much higher level of protection for the secure data (col. 1, lines 25-31).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within

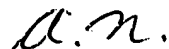
Art Unit: 2132

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

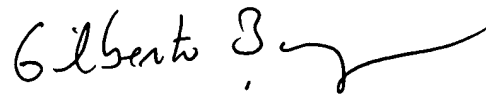
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

  
Abdulhakim Nobahar  
Examiner  
Art Unit 2132

AN  
May 25, 2004

  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100